10/038,017. Aeg 8/30/07

A 520 ~~504~~ or conditional access system B 524 or passed in the clear to the cable system 32. As previously, the program or SI encrypted according to the legacy CA system A can be properly decoded by STB 36. The CA system B encrypted information is understood by STBs 536 and decrypted and decoded accordingly, as described previously.

A24 cancel.

Please rewrite the single-row table on line 9 of page 37 to read:

A25

025C04	025E05	125E11	025C06	025C07	025C08	025C09	~~125E12~~ 025E10	125E12

Please rewrite the single-row table on line 20 of page 37 to read:

A26

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12

Please rewrite the single-row table on line 24 of page 37 to read:

A27

125C04	025E11	125E05	125C06	125C07	125C08	125C09	~~125E10~~ 025E12	125E10

Please rewrite the paragraph starting on line ~~24~~ 5 of page ~~38~~ to read: Aeg 8/30/07

The primary and secondary PIDs are conveyed to the STBs in the program map table (PMT) transmitted as a part of the program specific ~~system~~ information (PSI) data stream. The existence of a secondary PID can be established to be ignored by the STB operating under CA encryption system A (the "legacy" system), but new STBs operating under CA encryption system B are programmed to recognize that secondary PIDs are used to convey the encrypted part of the program associated with the primary PID. The set-top boxes are alerted to the fact that this encryption scheme is being used by the presence of a CA descriptor in the elementary PID "for loop" of the PMT. There typically would be a CA descriptor for the video elementary PID "for loop", and another one in the audio elementary PID "for loop". The CA descriptor uses a Private Data Byte to identify the CA_PID as either the ECM PID or the secondary PID used for partial scrambling, thus

A28

10/038,217 Reg 8/30/07

A32 concl. (e.g., NDS) ~~is~~ are immediately adjacent the legacy encrypted packet (or at least prior to next primary stream video packet) then the pruning of the legacy packet in effect accomplishes the merging of a single, clear stream into the header strip and video queue.

Please rewrite the paragraph starting on line 1 of page 46 to read:

A third technique for implementation of partial decryption in a set-top box is illustrated in **FIGURE 16**. In this embodiment, the PID remapping is carried out either within a circuit such as an Application Specific Integrated Circuit (ASIC), Field Programmable Gate Array (FPGA), or a programmable logic device (PLD) 938 or other custom designed circuit placed between the tuner and demodulator 904 and the decoder IC 908. In a variation of this embodiment, the decoder IC 908 can be modified to implement the PID remapping within demultiplexer 940. In either case, the legacy encrypted packets are dropped and the non-legacy packets are re-mapped either in circuit 938 or demultiplexer 940.

A33

Please rewrite the paragraph starting on line 24 of page 47 to read: 10 40 Reg 8/30/07

This third technique can be implemented in one embodiment using the PLD depicted in **FIGURE 17**. This implementation assumes that there will ~~be~~ not be more than one encrypted packet of a particular PID appearing in a row, thus, the implementation could be modified to accommodate bursts of encrypted packets such as with the M and Nth encryption arrangement described above (as will be explained later). The input stream passes through a PID identifier 950 which serves to demultiplex the input stream based upon PID. Primary PID packets are checked for continuity at 958. If a continuity error is detected, the error is noted and the counter is reset at 960.

A34